Criptografia e Protocolos de Segurança

MMAC, MEIC

Exame 1 - 14 val.

3 hours

Grupo I 1.0 + 2.0

1 Let $S = ((X, X, C, e, d), q_X, q_C)$ be a stochastic cryptosystem such that $|C| = 2|X|$. State a sufficient condition for S to be unconditionally secure and prove your statement.

2 Let (K, f) be a key stream (fluxo de chave) for $S = (X, X, C, e, d)$. Assume that there exists $c \in C$ such that $e_c(x) = d_c(x) = x$ and that for all $c_1, c_2 \in C$ there exists $c_3 = c_1 \circ c_2$ such that $e_{c_3}(x) = e_{c_1}(e_{c_2}(x))$. Show that $d_k^* \circ e_k^* = id_{X^*}$ for all $k \in K$. Describe how to compose key ciphers over S and give the key stream (K', f') that, when composed with any other stream cipher (K, f) over S, gives a stream cipher that behaves like (K, f).

Grupo II 2.0 + 2.0 + 3.0

1. Show that ElGamal signature scheme is sound. Show how to attack the scheme for Z_p when $p - 1 = 2^n$.

2. Propose a signature scheme such that: (i) the validity of the signature can be verified with a private verifying key u; (ii) the private signing key is divided among 3 signing parties, that is, there are 3 signing keys c_1, c_2 and c_3 such that $Ver_u(m, s) = 1$ iff $s = Sig_{c_1}(Sig_{c_2}(Sig_{c_3}(m)))$; (iii) $Sig_{c_i} \circ Sig_{c_j} = Sig_{c_j} \circ Sig_{c_i}$; (iv) it should be hard to obtain c_i having just one c_j; (v) the signing parties do not know u.

3. Consider the asymmetric (pseudo)cryptosystem $A = (Z_n, Z_n, C, e, d, Z_n, b)$ where $n = pq$ with p and q primes such that $p = 3 \mod 4$ and $q = 3 \mod 4$, $C = \{(p, q, B) : 0 \leq B \leq n - 1\}$, $b(p, q, B) = B$, $e_B(x) = x(x + B) \mod n$ and $d_{(p,q,B)}(y) = \sqrt{\frac{B^2}{4} + y} - \frac{B}{2} \mod n$.

a) Show that, by knowing p and q, it is possible to compute efficiently the square roots of a quadratic residue mod n.

b) Show that (i) e_B is not injective, (ii) $d_{(p,q,B)}(y)$ gives 4 decrypts; (iii) and if $y = e_B(x)$ then one of the decrypts is x.

c) Show that in the possession of an oracle O such that $O(y)$ is a solution for $d_{(p,q,B)}(y)$, it is possible to factor n in (bounded probabilistic) polynomial time (hint: use the fact that by knowing two random roots of a quadratic residue mod n it is possible to factor n with a positive probability).

Grupo III 2.0+2.0

1. Describe the Diffie-Helmann key distribution protocol and show how to attack it with the man-in-the-middle attack. Suggest a solution to make the protocol robust to this attack.

2. Describe the Ekert 91 protocol and discuss advantages of this protocol in comparison with Diffie-Helmann. Show that, when measuring a qubit of the EPR state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with the measurement $\{\cos(\theta)|0\rangle + \sin(\theta)|1\rangle, -\sin(\theta)|0\rangle + \cos(\theta)|1\rangle\}$, both qubits collapse in the same state.